Article

An Enhanced Approach for Three Factor Remote User Authentication in Multi - Server Environment

Dhara Joshi [1,†,‡], Chintan Patel [1,‡,*], Nishant Doshi [2], Rutvij Jhaveri[2], and Xianmin Wang[2]

[1] MEFGI,India; dhara.r.joshi@gmail.com
[2] PDPU,India; chintan.p592@gmail.com
[2] PDPU,India; doshinikki2004@gmail.com
[2] NTU,Singapore; rutvij.jhaveri@svmit.ac.in
[2] Guangzhou University, Chinta; xianmin@gzhu.edu.cn
* Correspondence: chintan.p592@gmail.com; Tel.: +91-7874182588
† Current address: Pandit Deendayal Petroleum University, Gandhinagar
‡ These authors contributed equally to this work.

Abstract: With quick improvement in the field of network, everything becomes online. Remote user authentication is a mechanism in which remote server verify the correctness of user over common or public channel. Remote user authentication can be Single server authentication or Multi server authentication. The disadvantage of single server authentication is that the user needs to recall user id and password for each service, he/she need to utilize, however it can overcome by Multi-server authentication in which user needs to register himself with Registration Center (RC) for the first run through and after that onwards he can utilize each service (which are given by servers, associated with RC) by recollecting only one user id and password. In this paper, we analyze Chen's authentication scheme (based on multi server authentication) and show that this scheme is vulnerable to password guessing attack, replay attack, RC spoofing attack, session key verification attack and perfect forward secrecy attack. In this Paper, we propose a biometric based remote user authentication scheme in multi-server environment. Proposed scheme is more secure and efficient as compared to chen's scheme[23].

Keywords: Multi-server, Smart card, Biometrics, Three factor authentication

0. Introduction

These days the popularity of web is expanding massively. Everything is accessible on web i.e. online services. In recent trends user does not go physically any place to get to a few services, but rather user remotely get to those services over web by giving his/her accreditation's. So users' information or data goes through unreliable or open channel. As all the correspondence and information exchange is done on open or basic channel, it is a major test to secure the information against various sorts of attacks. For that, system needs to authenticate (i.e. is the remote user who he/she claims to be) and authorize (i.e. is the remote user has rights to get to specific administration) the remote user. This preparing advancement is only Remote User Authentication plot. Conventional system for remote user authentication incorporates password table at server side, however these days the entire situation changes as Smart Card comes in the picture. Smart card is only a plastic card or pocket estimate card having inserted microchip that can be stacked with data or information. Smart card can used to give authentication, storage of information and so forth. Multi server authentication can be of any kind: Two factor authentication or Three factor authentication. It is comprehended why it is 2-factor authentication, 3-factor authentication and which parameters choose this factor in authentication. Authentication should be possible by underneath three parameters:

(1) What Remote user Know (Password, PIN)
(2) What Remote user Has (Mobile, RFID, Smart card, E-token)

 doi:10.20944/preprints201810.0151.v1

(3) Who Remote user is (Bio metrics)

In 1981, Lamport [1] presented password based validating the remote user over an open or regular channel. It had three issues, so for the arrangement of them it utilizes one path work for encoding the secret key. This framework stores the user's password at server side, such a large number of attacks are conceivable on this framework. Remembering the ultimate objective to deal with the authentication related issues and strengthen the security of the structure, smart card based authentication plans are presented.

To solve the issue of Lamport's plan in 2003, Aoshima et al [2] (US Patent - One time Logon Method) present the difference among authentication and authorization and they said in regards to one time password for diminish the danger of impersonation of password. Lee et al [3] proposed a remote user authentication scheme based on two factor authentications. In 2006, Cheng's scheme [6] gave brief idea about the interaction between multiple servers and end user device. It will be like multi server domain.

Some of the schemes [3–20] have the advantage like it needn't bother with any password table, rather they use Smart Card. In 1999, Hwang and Li [8] and Sun proposed a new authentication scheme using a smart card to improve the efficiency without using password table. But, these schemes don't permit remote users to uninhibitedly Select and update their passwords. In 2009, Xu et al [5] proposed Smart card based authentication scheme which based on the assumption that both user's password and smart card are not stolen by attacker. Suppose user's smart card is stolen by attacker and attacker doesn't know the password.

In 2006, Cheng's scheme [6] introduces a interaction of multiple server with end device. In order to cope up with the drawback of password table authentication and two factor authentication Li et al [8] proposed a three factor means biometrics-based authentication scheme in 2009. The scheme mutually authenticates both the communicating parties and rather using synchronized clock for preventing Replay attack, it uses random number.

All the scheme [1–23] having some security issues like some of the scheme are weak against password guessing attack, forgery attack, user impersonation attack and many more. As shown in above figure we analyze the different authentication schemes. Some of the recent schemes on new technologies are proposed in [24–31], [32–40], we recommend readers to study these.

So the primary issue is security concerns. In past plan, they utilize password table to stores the password at server side either in the plain content or in encrypted arrangement however then likewise a few attacks like server caricaturing or privileged insider can be conceivable. So to take out the issue of password table these days Smart card comes in the situation. Authentication data is put away inside the smart card and it will give ease approach to change your password all the more safely.

1. Review of Chen's Scheme

In this section, we will present a brief review of Chen's Scheme [23]. In his scheme, there are four phases mentioned:
1) Registration Phase
2) Login Phase
3) Authentication Phase
4) Password Change Phase.

1.1. Registration Phase

In this phase, User selects ID_i , PW_i and r. Identity of the user ID_i and Hashing of random number r and Password PW_i is sent over secure channel for User registration. Registration center perform some calculation. Here x and y is secret key generated by the RC. After performing the operations RC created smart card and passes it to user over secure channel.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 8 October 2018 doi:10.20944/preprints201810.0151.v1

Step 1: User computes h($r \oplus PW_i$) and sends ID_i and h($r \oplus PW_i$) over secured channel to the server.

Step 2: Server computes R_i = h(h($r \oplus PW_i$)), $M_i = h(R_i||h(x \oplus y))$, $E_i = M_i \oplus h(r \oplus PW_i)$, L_i=h($ID_i||x$), $W_i = L_i \oplus h(ID_i||h(r \oplus PW_i))$, F_i = h(L_i).

Step 3: Server generates smart card SC = {W_i,E_i,F_i,h(.),h(y)} and send it to user in secured manner.

1.2. Login Phase and Authentication Phase

In login phase, User inputs ID_i and PW_i. Then at user side some operation is performed and then user send parameter set $m1$ to the remote server for login purpose. In authentication phase, Server perform some operation to validate the user and send parameter $m2$ to the user. Now user verifies the server and send parameter set $m3$ to the server. Thus both the parties mutually authenticate each other and draws session key.

Step 1: User computes $L_i = W_i h(ID_i||h(rPW_i))$, F_i* = h(L_i) then check F_i* ?= F_i, if this is verified.

Step 2: User generates random number N_i and computes M_i= $E_i h(rPWi)$, R_i = h(h(rPW_i)), G_{ij} = $R_i h(h(y)||N_i||SID_j)$, CID_i = h(rPW_i)$h(Li||Mi||Ni)$, $H_{ij} = L_i h(M_i||Ni_||SID_j)$, Z_i = h($E_i||M_i||N_i$). and Sends message m1={CID_i, G_{ij}, H_{ij}, Z_i, N_i} to server on open channel.

Step 3: After receiving message from user server computes $R_i = G_{ij} \oplus h(h(y)||N_i||SID_j)$, M_i = h($R_i||h(x||y)$), $L_i = H_{ij} \oplus h(M_i||N_i||SID_j)$,h($r \oplus PW_i$) = $CID_i \oplus h(L_i||M_i||N_i)$,$E_i = M_i \oplus h(r \oplus PW_i)$, h($E_i||M_i||N_i$) ?= Z_i, Generates random number N_j and compute V_{ij} = h($E_i||N_i||M_i||SID_j$). Generates message m2 = {V_{ij},N_j} and send to user.

Step 4: User computes h($E_i||N_i||M_i||SID_j$) ?= V_{ij}, V'_{ij} = h($E_i||N_j||M_i||SID_j$). Generates message m3 = V'_{ij} and send it to server on open channel.

Step 5: Server receives message and computes h($E_i||N_j||M_i||SID_j$) ?= V'_{ij}, SK = h($E_i||N_i||N_j||M_i||SID_j$).

Step 6: User also computes session key SK = h($E_i||N_i||N_j||M_i||SID_j$).

1.3. Password Change Phase

In this phase, User can enter his/her credentials and after the validation he/she can change password without any interaction with server.

Step 1: User provides ID_i and PW_i than system computes $L_i = W_i \oplus h(ID_i||h(r \oplus PW_i))$,F_i* = h(L_i), and verifies F_i* ?= F_i Select $PW_{i_{new}}$, r_{new} and computes $W_{i_{new}} = L_i \oplus h(ID_i||h(r_{new} \oplus PW_{i_{new}}))$, $E_{i_{new}}$ = $E_i \oplus h(r \oplus PW_i) \oplus h(r_{new} \oplus PW_{i_{new}})$.

Step 2: Updates smart card SC = {$W_{i_{new}}$, $E_{i_{new}}$, F_i, r_{new}, h(.), h(y)}.

2. Cryptanalysis of Chen's Scheme

In this section, we analyzed the drawbacks of Chen's Authentication scheme[23].

*2.1. **Password Guessing Attack***

In Authentication phase, there is parameter called $V'_{ij} = h(E_i||N_i||M_i||SID_j)$. In this parameter the value of N_j (server nonce) can be intercept because it is in plain text in Second parameter Set $m2$, the value of

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 8 October 2018 doi:10.20944/preprints201810.0151.v1

SID_j (Server's identity) can be known to everyone, the value of E_i can be intercept if attacker get the Smart card (because smart card contains the parameter E_i). So we have only one parameter which is unknown, but $M_i = h(r \oplus PW_i) \oplus E_i$. So as per rules of X-OR if we have any of the two operands out of three, we can get the last one. Attacker tries new password PW_i' and if this password is correct one then from this Computation $M_i' = h(r \oplus PW_i') \oplus E_i$. We can get the right value of M_i. and thus we have all four correct values which is used in V_{ij}' so we get it correct and impersonation as genuine user.

2.2. *Replay attack*

Whenever attacker tries to send the same message which is intercepted before some time, it is called Replay Attack. In Chen's Scheme in authentication phase, if attacker intercept the first parameter set $m1 = CID_i, G_{ij}, H_{ij}, Z_i, N_i$ and send the $m1$ to server after a while. Server computes R_i, M_i , L_i , E_i and compare Z_i ?= $h(E_i||M_i||N_i)$ and then generates Server nonce N_j . if the user is not genuine then also server compute these much operation means eight time hash function and six XOR function after that it will know the user is legal one or not. It wastes the CPU resources and take more time for only verification of the user.

2.3. *RC Spoofing Attack*

If Registration Center act as attacker, then attacker has all the resulting values for which it will perform computation. So in Registration Phase RC has get resulting parameters R_i , M_i, E_i, L_i , W_i, F_i. Now we can think that in this scheme Session key can be computed in authentication Phase like $SK = h(E_i||N_i||N_j||M_i||SID_j)$, where N_i(user nonce) and N_j (Server Nonce) can be intercept from public channel, SID_j is known to everyone and rest of the parameters E_i and M_i can be got easily as it is at RC and RC is the attacker. So now attacker has all five parameters of Session key so it will impersonate as legal user.

2.4. *Perfect forward secrecy*

In Authentication phase, the value of $V_{ij}' = h(E_i||N_j||M_i||SID_j)$, thus it depends upon these four parameters. Among those four parameters only Nj (server nonce) is random number generated by server and is change every time otherwise for a particular user all values remain same if the user want to use service from one particular server. So we can say that V_{ij}' depends upon N_j. One possibility is like if by mistake server generates the same random number for N_j, then the value of V_{ij}' will be the same which is calculated at previous when the same N_j occurs. If $N_j = 1 \rightarrow V_{ij}' = 23$, if $N_j = 5 \rightarrow V_{ij}' = 42$ but if now $N_j = 1$ then it is surely V_{ij}' is going to be 23.

2.5. *Session key verification attack*

In Authentication Phase, Both the parties generate session key, $SK = h(E_i||N_i||N_j||M_i||SID_j)$ but session key is not verified, so it is not the right way to provide mutual authentication before starting the actual conversation. Before communicating messages session key should be establish and verified by both the parties.

2.6. *Performance issue*

Chen's Scheme is having too many hashing function. It will take more time to perform authentication. In registration phase 8 hash functions are available, in Login phase 9 hash functions, in authentication phase 9 hash functions and in password change phase 4 hash functions are available. So total 30 times hash operation is performed. So it occupies more time and decrease the performance.

3. Proposed scheme

In this Section, we proposed new approach for multi server authentication by adopting key agreement scheme using smart card. We apply three factor authentications in multi server

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 8 October 2018 doi:10.20944/preprints201810.0151.v1

environment. In new protocol, there are three phases:
A. Registration Phase
B. Login and Authentication Phase
C. Password Change Phase.

There are mainly three entities in our proposed algorithm:
A. Remote User
B. Registration Center
C. Server.

Three keys are generated by RC.
$KFH \rightarrow$ pre-shared key between RC and server,
$MSK \rightarrow$ secret key generated by RC for legal remote user,
$FSK \rightarrow$ secret key generated by RC for legal server, Where $KFH = h(ID_{Server}||FSK)$.

3.1. Registration Phase

New User can Register himself with RC(Registration Center) and access any of the servers associated with RC.

Step 1: User selects ID_i, PW_i, BM_i and random number r

Step 2: SCR computes $RPW_i = h(PW_i||H(BM_i))or RPW_i = h(PW_i||ID_i||r)$ then, SCR send Registration request (ID_i, RPW_i) to Registration Center over Secure Channel.

Step 3: RC Calculates $A_i = h(ID_i||MSK)$, $B_i = A_i \bigoplus RPW_i$, then RC send the reply with parameters $B_i, A_i, Ek(.)/Dk(.), h(.)$ to remote user over secure channel.

3.2. Login and Authentication phase

In this phase mutual authentication is performed and session key is generated and verified for further conversations.

Step 1: User enter ID_i, PW_i and BM_i

Step 2: SCR Computes $RPW_i = h(PW_i||H(BM_i))$ or $h(PW_i||ID_i||r)$ if $A_i \bigoplus RPW_i \stackrel{?}{=} B_i$. If not equal then the process is terminated here otherwise it performs next steps. Generate rMU and perform $RMU = rMU.P$, $D_i = EPUB_S\{RMU, A_i, B_i, T_1, ID_i\}$.

Step 3: Login request (D_i, T_1) send to Server.

Step 4: Server Computes If $T_2 - T_1 <= \Delta T$ $DSEC_S\{D_i\}$

Step 5: Server Send message to RC in encrypted format and the key is pre shared key KFH. So the sent message is $EKFH\{A_i, ID_i, T_3\}$ and then RC Computes $T_4 - T_3 <= \Delta T$, $DKFH\{A_i, ID_i$, If $h(ID_i||MSK) \stackrel{?}{=} A_i$.

Step 6: RC send the response to Server (T_5) and Server Computes $T_6 - T_5 <= \Delta T$, Generate rFA, $RFA = rFA.RMU$, $RPW_i = Bi \bigoplus Ai$, $Fi = RMU \bigoplus RFA$, $SK = h(RFA||ID_i||RPW_i||T_7)$

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 8 October 2018 doi:10.20944/preprints201810.0151.v1

Step 7: Server send response to remote user $(h(SK), T_7, F_i)$ and user Computes $T_8 - T_7 <= \Delta T$, Get $RFA = F_i \bigoplus RMU$, If $h(h(RFA||ID_i||RPW_i||T_7)) \stackrel{?}{=} h(SK)$

Step 8: SCR verify the Session key and Session key agreement is performed.

3.3. password change phase

User can directly change his password without any interference by RC or remote server.

Step 1: User selects ID_i, PW_i, BM_i

Step 2: SCR Computes $RPW_i = h(PW_i||H(BM_i))$ or $h(PW_i||ID_i||r)$, if $A_i \bigoplus RPW_i \stackrel{?}{=} B_i$. If not equal then the process is terminated here otherwise it performs next steps.

Step 3: User select new password PW_i^*.SCR Computes $RPW_i^* = h(PW_i^*||H(BM_i))$ or $h(PW_i^*||ID_i||r)$, $Bi^* = A_i \bigoplus RPW_i^*$.Then Smart card Stores the parameters $r, B_i^*, A_i, Ek(.)/Dk(.), h(.)$.

4. Security Analysis of Proposed Scheme

*4.1. **Password Guessing Attack***

In Password Guessing attack, attacker guesses and tries different passwords and attacker succeed to prove him/herself as genuine one. In our Proposed scheme, attacker can use $RPW_i = h(PW_i||H(B_i))$ or $h(PW_i||ID_i||r)$. So attacker can guess the password but he/she can't guess the RPW_i as RPW_i contains other parameters like Biometric of the user or Identity of the user and random number selected by the user. So attacker does not succeed to prove him/herself as genuine user.

*4.2. **Replay Attack***

If attacker store past login message and utilize that message to login in the server after some time and on the off chance that he/she can effectively login in the server then it is called replay attack. In our Proposed scheme we utilize time stamp in each message which are transmitted on open channel and check this time stamp at target place. So in our proposed method we perform two times verification for better security of the system.

*4.3. **Spoofing Attack***

In Registration Center (RC) Spoofing attack, RC is an attacker. That means whatever the parameters stored at RC at the time of registration is misused by attacker and tries to get Session Key from that stored parameters. In our proposed work, we generate Session Key $SK = h(RFA||ID_i||RPW_i||T_7)$. If RC became an attacker, then also it has value of only two parameters Ai and Bi. But we are not utilizing Ai and Bi in Session key parameters, So there is no any possibility of this attack.

*4.4. **Perfect Forward Secrecy Attack***

If user's credentials or any sensitive information are bargain then attacker effectively figure the session key, it is called Perfect Forward Secrecy attack. In our proposed scheme, we took care that our random number is directly not concerned as one of the parameter of verification procedure. We take one random number and then multiply it with another random number for more security and then multiply this value with another random number and the final result is one of the parameters of session key. Random numbers are rMU, P and rFA, We calculate $RMU = rMU.P$ then $RFA = rFA.RMU$.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 8 October 2018 doi:10.20944/preprints201810.0151.v1

And $SK = h(RFA||ID_i||RPW_i||T_7)$. Thus, our proposed scheme is strong enough against Perfect Forward Secrecy Attack.

4.5. *Session Key Verification Property*

In any of the system, Session key should be generated at both the ends and it must be verified by any of the end, if session key is verified then system achieves session key verification property. In our Proposed Scheme, Server generated $SK = h(RFA||ID_i||RPW_i||T_7)$ and in public channel it would be sent as $h(SK)$ and at user side it would be verified as $h(h(RFA||ID_i||RPW_i||T_7)) \stackrel{?}{=} h(SK)$. So, Proposed scheme accomplish session key verification property.

4.6. *User Anonymity Property*

At the point when user's identity is obscure to server, it is called User Anonymity. In remote server authentication user must be unidentifiable and untraceable. In our Proposed Scheme, Smart Card does not store user's identity. $SC = r, A_i, B_i, Ek(.)/Dk(.), h(.)$. If Smart card is compromised, then also identity of the user is not revealed. At Login time message does not contain user identity directly D_i, T_1 where $D_i = E_{Pub\_ser}\{RMU, A_i, B_i, T_1, ID_i\}$. Thus, proposed method achieves User Anonymity property.

4.7. *User Impersonation Attack*

In User Impersonation attack, attacker claims that he/she is the genuine user of the system. So for that attacker send login request to server and if server authenticate him/her then he/she can prove him/herself as legal user. In proposed scheme attacker cannot make login request D_i, T_1 where $D_i = E_{Pub\_ser}\{RMU, A_i, B_i, T_1, ID_i\}$ and here $Ai \bigoplus RPW_i = B_i$ and $RPW_i = h(PW_i||ID_i||r)$. So it is not possible to impersonate the legal user as the value of D_i depends on the identity, password, random number and MSK. So our proposed scheme is secure against user impersonate attack.

4.8. *Secure and User-friendly Password Change Phase*

In Proposed scheme, if user wishes to change his/her password then it is easy to perform. In Password Change Phase user enters his/her credentials like identity, password & random number / biometrics. Then Smart card verify the user if user is authenticated then user is allowed to enter new password PWi^* and compute the parameters $RPW_i^* = h(PW_i^*||H(B_i))$ or $h(PW_i^*||ID_i||r)$, $B_i^* = A_i \bigoplus RPW_i^*$. And then update the smart card with the updated parameter without connected with server or registration center.

4.9. *Denial Of Service Attack*

At the point when availability of the server is disrupted by attacker is called DOS attack. In our proposed scheme we uses Biohash function for the improvement of security and reduction in time. It is useful because in normal hashing function, if the input is biometric then avalanche effect of hash function took more resources for more time compared to Biohash function. In Base scheme, it uses more cpu resources to prove the legitimacy of the user but in our proposed scheme we perform less computational operation for the same authentication purpose. Thus we reduce the wastage of CPU resources.

4.10. *Smart Card Stolen Attack*

If the smart card of the genuine remote user is stolen by attacker then attacker tries to get all the parameters from that smart card, If attacker succeed then he /she will get access of user's account and this attack is called Smart Card Stolen attack. In our proposed scheme, if smart card is stolen then also attacker can't get value of $D_i = EPUB_S\{RMU, A_i, B_i, T_1, ID_i\}$ because $SC = \{r, A_i, B_i, Ek(.)/Dk(.), h(.)\}$. Thus, our proposed scheme withstands smart card stolen attack.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 8 October 2018 doi:10.20944/preprints201810.0151.v1

4.11. *Modification Attack*

If any of the messages passed in public channel is modified by attacker then it is called modification attack. In our proposed scheme, all the messages passed through public channel are in encrypted format or in hashing format, so only legal user or server can access those data or interpret it. So our scheme withstands modification attack.

4.12. *Session Key Computation Attack*

If attacker intercept and compute session key passed through public channel to get access in the system then it is called Session key computation attack. In proposed scheme, $SK = h(RFA||ID_i||RPW_i||T_7)$, thus it uses time stamp which is auto generated, $RFA = rFA.RMU$ which uses random number multiplication to improve the security. So every time time stamp and this random value are different so we can say that proposed scheme is secure against Session key computation attack.

4.13. *Mutual Authentication Property*

In Mutual Authentication both the parties authenticate each other, here in our proposed scheme RC authenticates both remote server and remote user by initially providing key MSK, FSK, KFH . In our proposed scheme, user encrypts data with server public key and if server is able to decrypt it with its secret key then mutual authentication between user and server is done then server encrypt data with pre shared key and sent to RC, if RC is able to decrypt it then mutual authentication between server and RC is done and RC authenticate user so user and RC is mutually authenticated. Thus, our proposed scheme follows mutual authentication property.

5. Performance Analysis

For comparison, we have used two parameters:
1) Based on Timing Operation
2) Based on Security Analysis
In first parameter, we proved that our proposed scheme takes less time as compared to Chen's scheme and in second parameter we proved that our proposed scheme is more secure against different attacks as compared to Chen's scheme.

5.1. *Analysis based on security*

Here in table 1, we compare chen's scheme and proposed scheme in terms of attacks. We consider the list of attacks and compare both the schemes against those attacks As appeared in underneath table, we demonstrated that our proposed scheme is better regarding security as proposed scheme is more secure when contrasted with Chen's scheme.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 8 October 2018 doi:10.20944/preprints201810.0151.v1

Scheme	Registration Phase	Login Phase	Authentication Phase	Password Change Phase	Total
Chen's Scheme [23]	$10T_h + 6T_x + 4T_c$	$11T_h + 9T_x + 9T_c + 1T_r$	$14T_h + 5T_x + 30T_c + 1T_r$	$7T_h + 6T_x + 2T_c$	$42T_h + 26T_x + 45T_c + 2T_r = 40.45ms$
Proposed Scheme	$2T_h + 1T_x + 3T_c$	$6T_h + 3T_x + 12T_c + 2T_r + 2T_m + 1E + 1D + 1AE + 1AD$		$2T_h + 2T_x + 4T_c$	$10T_h + 6T_x + 19T_c + 3T_r + 2T_m + 1E + 1D + 1AE + 1AD = 13.34ms$

Table 2. Comparison based on Timing

Attack	Chen's scheme	Proposed scheme
Password Guessing Attack	Insecure	Secure
Replay Attack	Insecure	Secure
Denial of Service Attack	secure	Secure
Stolen smart card attack	secure	Secure
RC Spoofing attack	Insecure	Secure
Modification attack	secure	Secure
Perfect forward secrecy attack	Insecure	Secure
User anonymity attack	secure	Secure
Session key verification attack	Insecure	Secure
User impersonation attack	Secure	Secure
Session key computation attack	Secure	Secure
Mutual authentication attack	Secure	Secure

Table 1. Comparison based on security

5.2. *Analysis Based on Timing*

Here in table 2, we compare chen's scheme and proposed scheme in terms of Timing. We took the time taken by hash function, exclusive or function, concate function, symmetric and asymmetric encryption/decryption function etc. and so forth to calculate the time taken by plan to confirm the remote user. As appeared in the underneath table, we demonstrated that our proposed work diminishes the overhead to validate the user when contrasted with base scheme.

6. Conclusions

we have analyzed different attacks in multi-server environment. We performed numerical analysis for Chen's authentication scheme. We found that his scheme is vulnerable to Password Guessing attack, Replay attack, Registration Center Spoofing attack, Perfect Forward Secrecy attack and Session Key Verification attack. We proposed scheme which is secure against the above specified attacks and other attacks. Thus, Proposed scheme provides more security and takes less time as compared to Chen's Scheme to authenticate the user.

References

1. C.T. Chen. Anonymity authentication method in multi-server environments. US Patent 9,264,425. 2016.URL:https://www.google.com/patents/US9264425.

2. Leslie Lamport. "Password Authentication with Insecure Communication". In: Commun. ACM 24.11 (Nov. 1981), pp. 770–772. ISSN : 0001-0782. DOI: 10 . 1145 / 358790 .358797.URL:

http://doi.acm.org/10.1145/358790.358797.

3. T. Aoshima, M. Tasaka, and K. Takeda.One-time logon method for distributed computing systems. US Patent 7,136,996. 2006. URL: http : / / www . google . tl / patents /US7136996.

4. NarnYih -Lee and Yu-Chung Chiu. "Improved remote authentication scheme with smart card". In: Computer Standards and Interfaces 27.2 (2005), pp. 177 –180. ISSN:0920-5489. DOI: https://doi.org/10.1016/j.csi.2004.06.001.URL: http://www.sciencedirect.com/science/article/pii/S0920548904000637.

5. R.C.H. Cheng, P.C. Van Oorschot, and S.W. Hillier.Sys-tems and methods providing interactions between multiple servers and an end use device. US Patent 7,010,582. 2006.URL: https://www.google.com/patents/US7010582

6. Muhammad Khurram Khan and Jiashu Zhang. "An Efficient and Practical Fingerprint-Based Remote User Authentication Scheme with Smart Cards". In:Information Security Practice and Experience: Second International Conference, ISPEC 2006, Hangzhou, China, April 11-14,2006. Proceedings. Ed. by Kefei Chen et al. Berlin, Hei-delberg: Springer Berlin Heidelberg, 2006, pp. 260–268.ISBN: 978-3-540-33058-5.DOI:10.1007/1168952224.URL: https://doi.org/10.1007/1168952224.

7. Jing Xu, Wen-Tao Zhu, and Deng-Guo Feng. "An improved smart card based password authentication scheme with provable security". In:Computer Standards and Interfaces 31.4(2009),pp.723–728.ISSN:0920-5489. DOI: https://doi.org/10.1016/j.csi.2008.09.006.URL:http ://www.sciencedirect.com/science/article/pii/S0920548908001165

8. C.T. Chen.Anonymity authentication method for global mobility networks . US Patent 9,021,265. 2015.URL: https://www.google.com/patents/US9021265.

9. Chun-Ta Li and Min-Shiang Hwang. "An efficient biometrics-based remote user authentication scheme us-ing smart cards". In: Journal of Network and Computer Applications 33.1 (2010), pp. 1 –5. ISSN: 1084-8045. DOI: https : / / doi . org / 10 . 1016 / j . jnca . 2009 . 08 . 001. URL: http : / / www. sciencedirect . com / science / article / pii / S1084804509001192.

10. [10] Xiong Li et al. "Cryptanalysis and improvement of a biometrics-based remote user authentication scheme us-ing smart cards". In: Journal of Network and Computer Applications 34.1 (2011), pp. 73 –79. ISSN: 1084-8045. DOI: https : / / doi . org / 10 . 1016 / j . jnca . 2010 . 09 . 003. URL: http : / / www. sciencedirect . com / science / article / pii / S1084804510001657.

11. Ankita Chaturvedi, Dheerendra Mishra, and Sourav Mukhopadhyay. "Improved Biometric-Based Three-factor Remote User Authentication Scheme with Key Agreement Using Smart Card". In: Information Systems Security: 9th International Conference, ICISS 2013, Kolkata, India, December 16-20, 2013. Proceedings. Ed. by Aditya Bagchi and Indrakshi Ray. Berlin, Heidelberg: Springer Berlin Heidelberg, 2013, pp. 63–77. ISBN: 978-3-642-45204-8. DOI: 10.1007/978- 3- 642- 45204- 8 5. URL: https://doi. org/10.1007/978-3-642-45204-8 5.

12. D. He and D. Wang. "Robust Biometrics-Based Authen-tication Scheme for Multiserver Environment". In: IEEE Systems Journal 9.3 (2015), pp. 816–823. ISSN: 1932-8184. DOI: 10.1109/JSYST.2014.2301517.

13. Xiong Li et al. "An enhanced biometrics-based user authentication scheme for multi-server environments in critical systems". In: Journal of Ambient Intelligence and Humanized Computing 7.3 (2016), pp. 427–443. ISSN: 1868-5145. DOI: 10 . 1007 / s12652 - 015 - 0338 - z. URL: https://doi.org/10.1007/s12652-015-0338-z.

14. M. Sarvabhatla, M. Giri, and C. S. Vorugunti. "Crypt-analysis of a robust and effective smart card-based remote user authentication mechanism using hash function". In: 2014 International Conference on Computer and Commu-nication Technology (ICCCT). 2014, pp. 123–128. DOI: 10.1109/ICCCT.2014.7001479.

15. Dheerendra Mishra. "Design and Analysis of a Provably Secure Multi-server Authentication Scheme". In: Wireless Personal Communications 86.3 (2016), pp. 1095–1119. ISSN: 1572-834X. DOI: 10 . 1007 / s11277 - 015 - 2975 - 0. URL: https://doi.org/10.1007/s11277-015-2975-0.

16. Morteza Nikooghadam, Reza Jahantigh, and Hamed Ar-shad. "A lightweight authentication and key agreement protocol preserving user anonymity". In: Multimedia Tools and Applications 76.11 (2017), pp. 13401–13423. ISSN: 1573-7721. DOI: 10.1007/s11042-016-3704-8. URL: https://doi.org/10.1007/s11042-016-3704-8.

17. V. Odelu, A. K. Das, and A. Goswami. "A Secure Biometrics-Based Multi-Server Authentication Protocol Using Smart Cards". In: IEEE Transactions on Informa-tion Forensics and Security 10.9 (2015), pp. 1953–1966. ISSN: 1556-6013.

18. Eun-Jun Yoon and Kee-Young Yoo. "Robust biometrics-based multi-server authentication with key agreement scheme for smart cards on elliptic curve cryptosystem". In: The Journal of Supercomputing 63.1 (2013), pp. 235– 255. ISSN: 1573-0484. DOI: 10.1007/s11227-010-0512-1. URL: https://doi.org/10.1007/s11227-010-0512-1.

19. Ming-Chin Chuang and Meng Chang Chen. "An anony-mous multi-server authenticated key agreement scheme based on trust computing using smart cards and biomet-rics". In: Expert Systems with Applications 41.4, Part 1(2014), pp. 1411 –1418. ISSN: 0957-4174. DOI: https :7/ / doi . org / 10 . 1016 / j . eswa . 2013 . 08 . 040. URL: http : / / www . sciencedirect . com / science / article / pii / S0957417413006611.

20. Azeem Irshad et al. "An efficient and anonymous multi-server authenticated key agreement based on chaotic map without engaging Registration Centre". In: The Journal of Supercomputing 72.4 (2016), pp. 1623–1644. ISSN: 1573-0484. DOI: 10 . 1007 / s11227 - 016 - 1688 - 9. URL: https : //doi.org/10.1007/s11227-016-1688-9.

21. A. G. Reddy et al. "A Secure Anonymous Authentication Protocol for Mobile Services on Elliptic Curve Cryptog-raphy". In: IEEE Access 4 (2016), pp. 4394–4407. ISSN: 2169-3536.

22. C. Shaik. Password self encryption method and system and encryption by keys generated from personal secret information. US Patent App. 12/402,786. 2009. URL: https://www.google.tl/patents/US20090296927.

23. L. Chen and S. Majumdar. Password-based cryptographic method and apparatus. US Patent 8,464,058. 2013. URL: https://www.google.com/patents/US8464058.

24. Han Shen et al. "New biometrics-based authentication scheme for multi-server environment in critical systems". In: Journal of Ambient Intelligence and Humanized Com-puting 6.6 (2015), pp. 825–834. ISSN: 1868-5145. DOI: 10.1007/s12652- 015- 0305- 8. URL: https://doi.org/10. 1007/s12652-015-0305-8.

25. Zhenxiang Chen et al. "Flexible neural trees based early stage identification for IP traffic". In: Soft Computing 21.8 (2017), pp. 2035–2046. ISSN: 1433-7479. DOI: 10.1007/ s00500 - 015 - 1902 - 3. URL: https : / / doi . org / 10 . 1007 / s00500-015-1902-3.

26. Q. Liu et al. "Preserving Privacy with Probabilistic Indis-tinguishability in Weighted Social Networks". In: IEEE Transactions on Parallel and Distributed Systems 28.5 (2017), pp. 1417–1429. ISSN: 1045-9219. DOI: 10.1109/ TPDS.2016.2615020.

27. Yi Liu et al. "Finger vein secure biometric template generation based on deep learning". In: Soft Computing 22.7 (2018), pp. 2257–2265. ISSN: 1433-7479. DOI: 10. 1007/s00500-017-2487-9. URL: https://doi.org/10.1007/ s00500-017-2487-9.

28. Tao Peng et al. "Collaborative trajectory privacy preserv-ing scheme in location-based services". In: Information Sciences 387 (2017), pp. 165 –179. ISSN: 0020-0255. DOI: https : / / doi . org / 10 . 1016 / j . ins . 2016 . 08 . 010. URL: http : / / www. sciencedirect . com / science / article / pii / S0020025516305801.

29. Wenbin Chen, Hao Lei, and Ke Qi. "Lattice-based linearly homomorphic signatures in the standard model". In: The-oretical Computer Science 634 (2016), pp. 47 –54. ISSN: 0304-3975. DOI: https://doi.org/10.1016/j.tcs.2016.04. 009. URL: http://www.sciencedirect.com/science/article/pii/S0304397516300378.

30. Haibo Tian and Jin Li. "A short non-delegatable strong designated verifier signature". In: Frontiers of Computer Science 8.3 (2014), pp. 490–502. ISSN: 2095-2236. DOI: 10.1007/s11704- 013- 3120- 4. URL: https://doi.org/10. 1007/s11704-013-3120-4.

31. J. Li et al. "Securely Outsourcing Attribute-Based Encryp-tion with Checkability". In: IEEE Transactions on Parallel and Distributed Systems 25.8 (2014), pp. 2201–2210. ISSN: 1045-9219. DOI: 10.1109/TPDS.2013.271.

32. Q. Lin et al. "An ID-Based Linearly Homomorphic Sig-nature Scheme and Its Application in Blockchain". In: IEEE Access 6 (2018), pp. 20632–20640. DOI: 10.1109/ ACCESS.2018.2809426.

33. R. H. Jhaveri et al. "Sensitivity Analysis of an Attack-Pattern Discovery Based Trusted Routing Scheme for Mo-bile Ad-Hoc Networks in Industrial IoT". In: IEEE Access 6 (2018), pp. 20085–20103. DOI: 10.1109/ACCESS.2018. 2822945.

34. Chen Wang et al. "A Novel Security Scheme Based on Instant Encrypted Transmission for Internet of Things," in: Security and Communication Networks 2018 (2018), pp. 10179–10188. DOI: https : / / doi . org / 10 . 1155 / 2018 / 3680851.

35. W. Meng et al. "When Intrusion Detection Meets Blockchain Technology: A Review". In: IEEE Access 6 (2018), pp. 10179–10188. DOI: 10.1109/ACCESS.2018. 2799854.

36. Jian Xu et al. "Dynamic Fully Homomorphic encryption-based Merkle Tree for lightweight streaming authenticated data structures". In: Journal of Network and Computer Applications 107 (2018), pp. 113 –124. ISSN: 1084-8045. DOI: https : / / doi . org / 10 . 1016 / j . jnca . 2018 . 01 . 014. URL: http : / / www. sciencedirect . com / science / article / pii / S1084804518300286.

37. Li Yang et al. "A remotely keyed file encryption scheme under mobile cloud computing". In: Journal of Network and Computer Applications 106 (2018), pp. 90 –99. ISSN: 1084-8045. DOI: https://doi.org/10.1016/j.jnca.2017.12. 017. URL: http://www.sciencedirect.com/science/article/pii/S1084804517304241.

38. Hongyang Yan et al. "Centralized Duplicate Removal Video Storage System with Privacy Preservation in IoT". In: Sensors 18.6 (2018).

39. Zheli Liu et al. "Cloud-based electronic health record sys-tem supporting fuzzy keyword search". In: Soft Computing 20.8 (2016), pp. 3243–3255. ISSN: 1433-7479. DOI: 10. 1007/s00500-015-1699-0. URL: https://doi.org/10.1007/ s00500-015-1699-0.

40. Zhaoquan Cai et al. "Towards Secure and Flexible EHR Sharing in Mobile Health Cloud Under Static Assump-tions". In: Cluster Computing 20.3 (Sept. 2017), pp. 2415– 2422. ISSN: 1386-7857. DOI:

10.1007/s10586-017-0796-5. URL: https://doi.org/10.1007/s10586-017-0796-5.

Sample Availability: Samples of the compounds ..... are available from the authors.